Annual Security Refresher Briefing

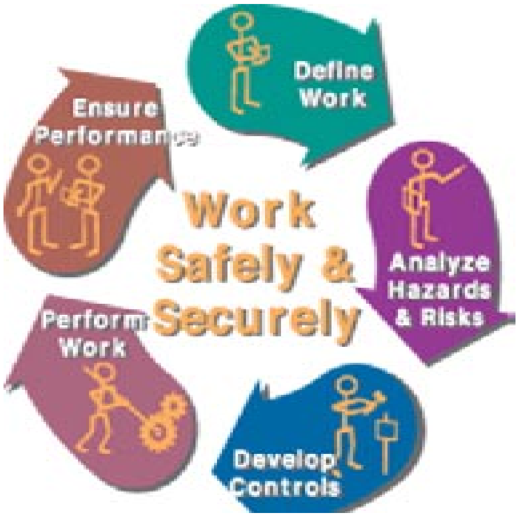
DEPARTMENT OF ENERGY • UNITED STATES OF AMERICA

NNSA
National Nuclear Security Administration

INTRODUCTION:

Hello, and welcome to the Annual Security Refresher for the Los Alamos National Laboratory. This briefing includes information on general security, classified matter protection and control, computer security, escorting, technical surveillance countermeasures, and operations security. By completing this training, you will have satisfied the following training requirements:
Annual Security Refresher-required for all active clearance holders.
Annual Computer Security Refresher-required for all computer users.
Technical Surveillance Countermeasures-required annually for all active employees at the Laboratory.

The purpose of this briefing is to make Lab employees aware of their individual security responsibilities. We have found that when people become aware they become more alert and increased alertness leads to fewer safety and security incidents. Remember, security is your responsibility. All employees holding a DOE clearance are REQUIRED to take the Annual Security Refresher every year. A notice will be sent to employees 60 days before, 10 days before, and the day of training expiration. If an employees training expires, Personnel Security will be notified to take appropriate action up to, and including, making a recommendation to DOE/AL that the security clearance be terminated.



A major part of security at the Lab is ISSM, Integrated Safeguards and Security Management. ISSM is a system for performing work securely, a way of doing business. ISSM provides a framework to support Lab workers in fulfilling his/her security responsibilities so that we do not compromise the security of our nation while satisfying the security requirements that have been put forth by the US-DOE contract.

Before we get started I would like to make you aware of security resources that are avaiLable to you. Should you have any comments, questions, or concerns that are related to security, please call the Security Help Desk. The Security Help Desk is there to provide you with any type of security guidance. The Security Help Desk can be reached at 665-2002. Much of this briefing data came from feedback and improvement suggestions to the Security Help Desk. We will collect your feedback and improvement suggestions on this briefing to incorporate into next years briefing.

Nuclear Safeguards
Classified Security
General Security

Secondly, LANL has developed an integrated set of three security Laboratory Implementation Requirements or LIRS. Currently we have three LIRs - General Security, Classified Security, and Nuclear Safeguards. Should you have any questions related to security policies or procedures, access the LIRs, which are located on Security's homepage. Over the course of the year, the LIRs will be migrating into new formats and content groupings based on the work being done. The new guidance documents will be able to be found on the Laboratory Policy webpage and the Security webpage.

Other valuable security resources include your Division Security Officers (or DSO) and your Organizational Computer Security Representatives or OCSR. If you have any general or computer security questions you may call upon your organization's DSO or OCSR. Lets begin by reviewing general security requirements.

GENERAL SECURITY REQUIREMENTS

One of the most frequent security incidents here at the Laboratory is the introduction of personal cell phones into security areas. Personal cell phones are NEVER allowed into security areas. A government owned cell phone or two way pager may be brought into a security area as long as the battery is removed from the phone/pager and remains out the entire time you are in that security area. Before you can use either your personal cell phone or government cell phone, or two way pager you must be outside the perimeter of that security area and at least 50 feet or more from any classified processing. Again, personally owned cell phones are never allowed in security areas, even with the battery removed. However, personal cell phones may be used in property protection areas and on Laboratory roads, parking lots, or other land that is routinely open to the public. Personal cell phones are not allowed into security areas for a variety of reasons. The number one reason is that cell phones have the ability to transmit information even when they are turned off. Cell phones also have the capability to be set to answer incoming calls automatically after a certain number of rings. I am sure you can imagine the security risks associated with this type of feature. And lastly, technology has progressed since the introduction of the first cell phone. Cell phones are not just phones anymore. They have picture, video, and web-browser capabilities.

In addition to cell phones, any type of personal electronic device like two-way pagers, or personal digital assistants, such as Palm Pilots are not allowed in security areas. Privately owned cameras, video recorders, tape recorders, or any item that has recording capabilities may not be brought into a security area.

There are certain requirements that must be followed by individuals who have been granted a DOE security clearance. Among them are reporting requirements which have recently changed. If any of the following scenarios happen to you, they must be reported immediately to S-6 Personal Security.

- Any arrests, including charges that have been dismissed
- Any warrants or restraining orders that have been placed against you
- Any detention by federal, state, county, or municipal authorities
- Any traffic violations for which a fine of $250 or more was imposed
- Use or involvement with illegal drugs
- Close and continuing contact with a citizen from a sensitive foreign country
- When approached by or contacted by someone who is seeking classified information
- When an individual is on leave of absence or extended leave for longer than 90 days
- Legal name changes
- Business association with a sensitive foreign country
- Bankruptcy or garnishment wages
- Treatment for drugs, alcohol, or mental illness is the new reporting requirement and must be reported

Over the last year there have been numerous questions as to when individuals should or should not wear their badge. Your badge identifies you as a Laboratory worker. It can tell an informed observer whether you are a DOE or contract employee, if you hold any type of clearance, and if you are in Human Reliability Program. Why make the job of someone trying to acquire information about you or the Laboratory any easier? That is why we ask that you make sure you take your badge off while not on Laboratory owned or leased property. Guidance from NNSA states that Lab workers must remove their DOE badge while not on Laboratory owned or leased property. Recently, Laboratory workers have asked if it is appropriate to wear your badge at the Motorola building and the answer is yes, as the Motorola building is Lab-leased space. It is equally important to make sure that you are wearing your badge while on Lab property. Your badge must be suspended between your neck and waist with your photo facing out so that our Security Police Officers know that you have legitimate business at the Lab. When your badge is not in use, ensure that you store it where it is safe from damage or theft. Loss or theft of a badge must be reported in person to the Badge Office within 24 hours OR the next business day.

If you are going to be escorting someone in the near future, please be aware of the requirements for doing so. The person that you are escorting must have official business here at the Lab. When escorting, ensure that you have filled out the Escort Log, as Form 1812 is no longer in existence. Each organization has their own escort log. Some are on-line while others may be using a paper and pencil log. It is the escort's responsibility to ask the escortee what their citizenship may be. If they say something other than the US, different requirements must be followed.

Reasons that are not valid for escorting are allowing uncleared into a security area to participate in social events or allowing someone known to have a suspended or revoked clearance access to a security area.

Anyone hosting a visit to limited security areas in the TA-3 Limited Area Complex are expected to use the new logging form called the "SM-43 Limited Area Complex U.S. Citizens Escort Log" avaiLable online. This is a site-specific log. Not all organizations have a web-based escorting log. If you have further questions regarding escorting call the Security Help Desk or access the Escort Training on-line.

Working with classified information also has certain requirements. If you are going to be working with classified matter, you are required to take the on-line course 16028, which is a general overview of classified matter protection and control. If you feel that you would like more in-depth information regarding this topic, you can take a live class, course 5646, which is offered once a month.

There are also certain requirements that must be followed when working with Classified Removable Electronic Media. Whether or not you are working with documents, CREM, or anything else that is classified you are required to report the loss or potential loss or any anomaly associated with classified matter to your Responsible Line Manager (RLM) and the Security Inquiry Team (SIT) immediately. Do not discuss the incident itself on the phone - only report that an incident has occurred and arrange for a secure location to discuss particulars.

Classified information is defined as any information that requires protection against unauthorized disclosure to avoid damage to national security. We more commonly use the term classified matter, which is an all-encompassing term to include documents, parts, and/or media, which may contain or reveal classified information.

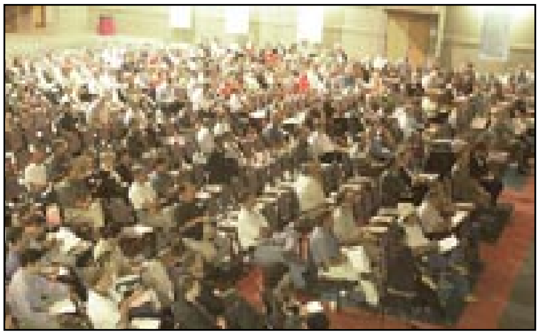
To help protect our classified matter we must make sure two requirements are met. First, your clearance level must be commensurate with the classified document level and secondly, you must have a need to know.

Need to know is a determination made by the authorized holder of that classified matter that an individual with the proper clearance level requires access to in order to perform or assist in tasks that are essential to a project or job they have been assigned. Always remember that all work involving classified information must be conducted only in approved security areas. Classified matter must not be left unattended at any time. When not in your physical control it must be stored in an approved GSA safe, vault, or vault-type room.

In order for a document to be classified, it must be assigned a classification level and category. The classification level and category tells us the extent of protection the classified matter needs. The classification level represents how much our national security could be damaged if the information were to be released. We have three levels of classified information: Top Secret, Secret, and Confidential. Top Secret information can be expected to cause exceptionally grave damage to our national security if the unauthorized disclosure happened to take place. Secret can be expected to cause serious damage, and confidential can be expected to cause damage. The classification category describes the type of information.

We also have three categories. Restricted Data, Formerly Restricted Data, National Security Information. Restricted Data deals with information that is related to the design, manufacturing, and testing of our nuclear weapons. Formerly Restricted Data is information that pertains to the military utilization of our atomic weapons, and National Security Information is all other information that does not contain nuclear weapons related information.

If your work may involve classified information, it is your responsibility to understand which information is classified and to properly protect such information. Your line manager and your organization’s Derivative Classifiers , or ADC’s, can assist you with this. You can find a list of ADCs on the web.



Also, regardless of the work you do, all of the material you produce that is intended for public release, such as professional journal articles, conference proceedings or posters, open web postings, and formal or informal reports, must be submitted for review and release by the Classification Group (S-7) before leaving the Laboratory. If you have any questions, contact S-7, at 667-5011.

The bottom line is to ensure you use the services of your ADC, or the Classification Group (S-7), BEFORE you transmit or share technical information which may be classified.

You must always obtain an official Los Alamos publication identification number for all work presented outside of the Laboratory. A LA-UR (" or Unlimited Release") is assigned to documents and other materials that are to be released to the public. You must submit an abstract or summary for all technical talks presented outside of the Laboratory on unclassified subjects. LA-URs can be anything from a one-paragraph abstract to a 1,000-page report being sent to a reading room for public avaiLability. There are five steps to follow for a LA-UR submission:

- First - complete the Technical Information Release form (Form 678) avaiLable online,
- Second- complete a cover sheet (Form 836), avaiLable through stock (ST-2629) or online. This cover sheet is required because of the legal statements printed on the bottom.
- Third - If you are sending audio-visuals such as videotapes that are to be returned through S-7, you must attach an abstract describing the subject for S-7 retention.
- Fourth - Send the completed Technical Information Release form 678; cover sheet form 836, and three copies of all full papers, or two copies of abstracts to S-7. See the Distribution of Los Alamos Publications for more information.
- Fifth - Allow three working days for processing. If you have any questions, contact S-7, Publications Release, at 667-5013.

Unclassified Controlled Information or UCI refers to information in which the disclosure, loss, misuse, alteration, or destruction could adversely affect national security. There are several different types of UCI. Unclassified controlled Nuclear Information (or UCNI) and Official Use Only (or OUO) are the most common.

UCNI is sensitive government information that is controlled even though is not classified. You do not have to hold a clearance to view UNCI but you must have a need to know. Security measures taken to protect UCNI transmissions must deter access by unauthorized individuals and restrict public release. UCNI must be protected by an approved encryption method when transmitted over public switched broadcast communications paths such as the Internet. UCNI may be transmitted by email without encryption if the sender and receiver are behind the LANL firewall. For more information about encryption requirements refer to General Security LIR, Attachment 11; Unclassified Information Systems Security.

OUO is applied to information that is unclassified yet exempt from release to the public under the Freedom of Information Act. In general, this information consists of sensitive administrative or personal information that warrants protection from unauthorized disclosure. Markings are not required for documents containing OUO information. Documents with OUO information may be marked: on the bottom of the front page or cover page and on each interior page or each interior page containing OUO information, with the legend; OFFICIAL USE ONLY. For more information about Unclassified Controlled Information, see the Security website "Protecting Information" or contact the Security Help desk at 665-2002.

CLASSIFIED REMOVABLE ELECTRONIC MEDIA

Over the last several years, LANL has had several incidents involving the mishandling of Classified Removable Electronic Media , known as CREM. As a result, the Department of Energy, National Nuclear Security Administration, and LANL have issued new directives and procedures for handling accountable CREM. CREM is a piece or item of removable computer media used to store classified information.

UC and LANL have developed a two-part definition of CREM. The first part defines classified electronic media as: those materials and components manufactured to provide nonvolatile storage of classified digital data that can be read by a computer. The second part defines removable as meeting one or more of the following criteria: designed to be introduced to and removed from the computer without adverse impact on computer functions, or separated from the computer for any reason, or portable electronic devices. Portable means a laptop, notebook, palm-type, or tablet computer, but not a desktop computer.

Examples of Removable electronic media are:

- Removable hard drives
- External hard drives
- Portable computers (laptops, notebooks, and tablets) that contain nonremovable hard drives and are accredited for classified processing
- Floppy diskettes
- Compact disks and Digital video disks (DVDs)
- Jaz, Zip, and PocketZip disks; Bernoulli cartridges; LS-120 disks, and other high-capacity removable disks
- USB "pen drives," flash drives, memory sticks, compact flash cards, and other solid state memory media
- AIT, DAT, DLT, QIC, or other magnetic or optical tape media used to store digital data
- Digital cameras with any non-removable memory

To ensure that LANL work involving accountable CREM is conducted in a safe and secure manner the Laboratory has established classified media libraries (CML) and classified library custodians (CLC). Think of CMLs as traditional libraries, and the CLC's working in those libraries. All accountable CREM is now in a CML. Before you can check out a piece of accountable CREM, your name must be listed on the Access Authorization list, or borrower list, provided to the CLC by your responsible-line manager. The borrower, the person who "checks out" a piece of accountable CREM, is solely responsible for the accountable CREM the entire time it is checked out of that library.

Keep in mind you must protect, store, and handle this piece of accountable CREM in accordance with Classified Matter Protection and Control requirements. As a prerequisite, all individuals who "borrow" accountable CREM and their responsible line managers must be formally trained by taking course #31411, "Accountable CREM RLM and Borrower Training."

CREM is created when a piece of media is inserted into a classified computer. That piece of CREM becomes accountable if the media is placed in the read/write drive of a classified computer system that is accredited for Secret Restricted Data or if the information put on the media falls under one of the accountable CREM categories, which ever is higher.

If a piece of accountable CREM happens to be produced, the person who produces it must protect, mark, and handle it correctly. The individual who produced the accountable CREM is now responsible for taking that piece of accountable CREM to his or her CLC to have a barcode placed on the accountable CREM and entered into the accountability system. This must be done by close of business the day the item was created. If it was created after hours then it must be done by COB the following day.

Keep in mind that CREM Secret/Restricted Data and above is considered accountable, as well as Sigma 14 and 15, Designated Special Access Programs, CRYPTO/COMSEC, Secret Foreign Government Information (FGI), including: Secret and Confidential United Kingdom (UK) "Atomic", Secret and Confidential North Atlantic Treaty Organization (NATO) "Atomal", SUCI (Sensitive Use Control Information), and classified media deployable for NEST/ARG, SECRET level matter not in any category above but processed, handled, and/or stored outside a security area (LA, EA, PA, MAA), Media containing SAP or COMSEC are accounted for by using programmatic guidance or other rules established by the program or agency responsible for the information.

Accountable CREM may not be destroyed locally (in your work area). All accountable CREM to be destroyed must be sent to the Classified Staging and Storage Center.

CYBER SECURITY

Every computer user is a link in LANL's cyber security chain, and all information has value. Always protect information from unauthorized access. The Cyber Security website and your O-C-S-R., Organizational Computer Security Representative, commonly referred to as an OSCAR, are valuable resources to refer to when you are working with Lab computers.

To protect you and your computer from the majority of threats, minimum computer protections include:

- Use computer resources for official use only and never for pornography, gambling, music downloading, or other inappropriate activity.
- Ensure that all software is licensed and that you are following all licensing agreements.
- Install virus protection and update it regularly.
- Follow established Laboratory password guidelines.
- Back up your files regularly.
- Enable password-protected screen savers when you're away from the computer.

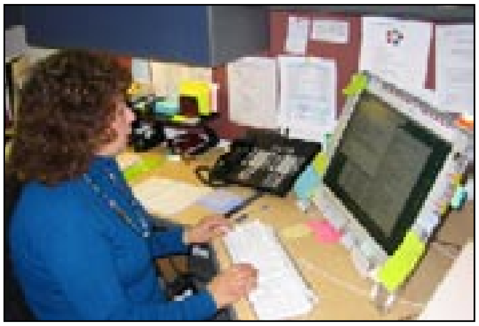
In order for foreign nationals to have computer access, some requirements must be met. The hosts of the foreign visitors and assignees must obtain pre-approval from management and the Foreign Visits and Assignments Office. The Laboratory host must complete both Form 982, for general access, and Form 982CA for computer access. The security plan must document the risk assessment and identify access controls. Remember that a foreign national is only allowed computer access that is approved on the 982CA. If access requirements change, the 982CA may need to be modified and resubmitted.

When a computer changes ownership, follow the guidelines and procedures of the Property Management Manual. Equipment should never be transferred without property accountability. If you need assistance in marking and protecting media, or getting a system accredited for use, consult your OCSR or S-11, Information Security.

Processing classified information has some serious risks. These include access by unauthorized users, breaches of security mechanisms such as passwords and firewalls, and disclosure or loss of information. It is your responsibility to protect the classified information you process at all times. Systems must not be used to process classified information until DOE has accredited the system.

The system must be operated according to the security plan and significant changes to the system require re-accreditation of the system. Access to a classified system depends on two things: your clearance level and your need-to-know. You must have both the proper clearance level and a need-to-know the information before access can be granted.

Cyber security incidents disrupt cyber resources. These incidents include physical damage to resources, interfering with software or applications, introducing malicious code, unclassified system contamination, and unauthorized access. All potential cyber security incidents should be reported to your OCSR. Classified information cannot be processed on an unclassified system. If an unclassified system is contaminated by classified information, then the system must be unplugged from the network. The system must be protected and the incident needs to be reported immediately to your OCSR or the Cyber Security Team.



Because computer technology is ever changing, new questions regarding cyber security come up all the time. We must be continually mindful of new threats posed to our cyber resources. Here are some tips in this ever-changing environment. The Cyber Security Team (cybersecurity@lanl.gov) is avaiLable to address your specific questions.

The use of wireless technology is restricted. Wireless capabilities being brought into Limited and Exclusions Areas must be disabled. Infrared (IR) wireless keyboards are allowed; radio frequency (RF) keyboards are prohibited. Wireless mice (IR and RF) are allowed. Wireless LANs must be pre-approved by DOE and are generally prohibited in Limited and Exclusion Areas except in safety-related applications.

Be careful when dealing with email. Never open an attachment in an email message that just doesn't make sense. Spam, unsolicited "junk" email sent to large numbers of people to promote products or services, is a growing problem. A spam filtering system has been implemented on the CCN-managed email servers that work very well in blocking most of LANL's spam. If you're not on a CCN-managed email server, you can use a filter on your own email application or just delete the messages. Of course, if you receive anything that really seems suspicious, report that to your OCSR. Remember that deleting an email message does NOT always delete the attachment. You must find where your email system stores attached files and delete them from there.

"Phishing" is another large problem. Phishing is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. There are several recent instances of a phishing scam in which users received emails supposedly from Citibank claiming that the user's account was about to be suspended. The email instructs the recipient to click on the provided link and update the credit card. Our institutional spam filters are now catching a lot of this phishing. If you get email asking for private information, do NOT respond. If it's a legitimate request, the company will contact you in other ways. Messages containing viruses are stripped of the virus and forwarded to the recipient indicating that a virus had been received and stripped. If you receive such a message, just delete it. If a virus is introduced into LANL's email network without being caught by the email servers, please contact your OCSR immediately. Again, be sure to NOT open up attachments on unknown email messages.

TECHNICAL SURVEILLANCE COUNTERMEASURES

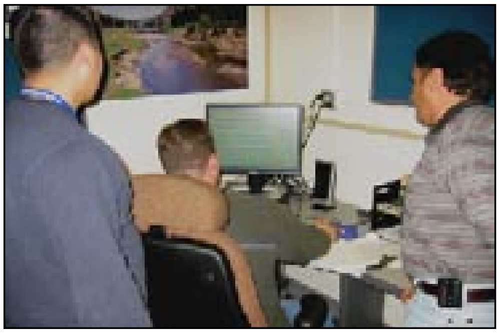
The Technical Surveillance Countermeasures, TSCM are those measures taken to detect and deter espionage; protect against inadvertent disclosure of classified or sensitive information; and protect your privacy at work. TSCM technicians use several techniques and a variety of electronic and electrical equipment to detect illegal devices designed to listen and or transmit information, more commonly know of as "bugs".

Some areas here at the Lab receive routine TSCM support. Those areas know and understand the importance of the TSCM program. However, just because your area does not receive this type of support does not mean that you do not have to worry about TSCM problems like bugs and taps! Illegal surveillance devices can be and have been used for many purposes other than collecting classified information.

The TSCM threat can come from two areas: the outside and the inside. Information on multi-million dollar contract negotiations and personal information that would be important in such things as promotions or divorce cases have been targeted in the past. In the event that you suspect or become aware of a technical surveillance penetration, you need to know the proper procedures for protecting and reporting the incident. First, stop all classified discussions and activity in the area. Protect the area so that no one can remove the suspected device. Immediately report the incident to your RLM and the TSCM Team, but do not call from your area or a nearby area, which may compromise the fact that there is a device in that area. Do not discuss details over the phone, simply state that you need to talk to them immediately. When the appropriate people arrive brief them about the situation outside of the area. And remember that the incident itself is classified and should not be discussed with those who do not have a need-to know.

OPERATIONS SECURITY

It is very important to note that there will always be adversaries from whom we must protect our vital secrets. That is why we practice Operations Security, otherwise known as OPSEC. This is a countermeasures program designed to disrupt or defeat the ability of foreign intelligence or other adversaries to exploit sensitive activities or information. Basically, giving away sensitive or unclassified information may lead our adversaries to information that may exploit our vulnerabilities. Keep in mind that even though you are giving out unclassified information, you may be helping adversaries gain the information they need. Bits and pieces of information they receive may be unclassified, but collectively they can be classified, and we want to protect against any compromise of classified or sensitive information.



Los Alamos National Laboratory plays a key role in our nation's defense and security, and because you are an employee of this Laboratory, you can become a target of a hostile foreign intelligence service or terrorist group. The hostile intelligence threat is a very real one. The threats can come from espionage, outsiders, or insiders. It is not beyond the realm of possibility that someone is trying to acquire information from you. Unexpected requests for information, often in the form of a thesis request, conversations being channeled into sensitive subject areas, or personal offers of paid travel for technical presentations may be "red flags" that could indicate that you are being targeted for espionage.

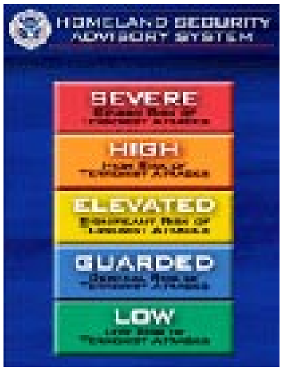
Please remember that if you are going on travel to a sensitive foreign country for personal as well as business, it must be reported to the ISEC office. Presidential Decision Directive/NSC-12 requires employees to report any attempts by unauthorized person to gain access to classified or otherwise sensitive information to the ISEC Office. The reporting requirement is not limited to sensitive or non-sensitive country foreign nationals, but rather pertains to attempts by any unauthorized person, even U.S. citizens.

Despite the end of the Cold War, foreign intelligence services are still tasked with gathering information. The foreign intelligence threat is a global problem and several countries are interested in our information.

They continue to target employees with scientific and technological backgrounds, high-profile research and development entities, as well as employees with access to National Laboratories. Many countries still have a need to enhance their military capabilities to ensure their own protection. Therefore, technologies that can enhance military capabilities are very valuable, particularly if these technologies and related information can be obtained through clandestine means, at little expense to themselves and their country.

The information and resources obtained could be utilized to damage the national security of the United States and advance their own capabilities or causes. The Department of State is deeply concerned about the continued threat of terrorist attacks against U.S. citizens and interests abroad, as well as the potential for demonstrations and violent actions against U.S. citizens and interests overseas. U.S. citizens are reminded that demonstrations and rioting can occur at any time. U.S. citizens are reminded to maintain a high level of vigilance and to take appropriate steps to increase their security awareness.

NEW SECURITY INITIATIVES



I am sure all of you are aware of the Labs Security Condition Levels (SECON Level) that are directly correlated to the Homeland Security Office threat levels of red, yellow, and orange. Whenever Homeland Security raises their threat levels our security measures raise as well.

Pajarito road has been closed to badge holders only. We have Security Posts located at the east and west ends of the Pajarito corridor. Individuals must stop and provide their security credentials to the Security Police Officers staffed at the post. There is restricted access beyond the two SECON access control posts on Pajarito Road. At least one person in all vehicles must possess a valid Laboratory/DOE security badge. Bicyclists must also stop at the SECON post and present a valid Laboratory/DOE Security badge. All other occupants over the age of 18 must possess either a valid Laboratory/DOE security badge or valid photo ID. "Vouching" for occupants over the age of 18 who do not have either a valid Laboratory/DOE security badge or valid photo ID will no longer be allowed. However, vehicle occupants under the age of 18 may be vouched for. All Laboratory/DOE badges or valid photo identifications must be touched by a protective force member when stopped at a security post.

Remember, Security is a must, in accomplishment of your responsibilities we trust! To receive credit for completing this briefing, click on the “Receive Credit” button below or fill out the form and return it to the Security Registrar. Thank you and have a safe and secure day.

BRIEFING ACKNOWLEDGEMENT

I certify I have read the Los Alamos National Laboratory’s Security & Safeguards 2005 Refresher Briefing. The contents of this briefing will be updated annually. If you print this briefing for usage throughout the year you are responsible for assuring you have the most current version. Credit will not be provided if the most current briefing content was not read. The last update of this briefing was March 25, 2005.

OPTION 1 - Online Credit Submission
If you have a Cryptocard with adminstrative access you can submit for credit using the “Receive Credit” button and your training record will be updated within the hour. If you do not have a Cryptocard, you must submit for credit to the S Division Registrar. Crediting of your training record will be completed within three days or sooner.

Receive Credit

OPTION 2 - Fax or Mail
Please allow up to 5 working days before credit will appear in Employee Development System (EDS) database if faxing or mailing this form.

Z #

Name – printed

Signature

Date

Phone Number

Please fax to:
(505) 665-8984
Or mail to:
S-Division Registrar
PO Box 1663
Mail Stop K560
Los Alamos, NM 87545